What is claimed is:

1. A terminal apparatus that communicates with another terminal apparatus on a network, the terminal apparatus possessing a public key of a group formed on the network, comprising:

an inquiry information sending unit operable to send inquiry information to said another terminal apparatus, the inquiry information indicating an inquiry about whether or not said another terminal apparatus is a terminal apparatus of an authorized member of the group;

an encrypted information receiving unit operable to receive predetermined encrypted information from said another terminal apparatus in response to the inquiry information sent by the inquiry information sending unit;

a decryption trial unit operable to try decrypting the received encrypted information using the group public key;

an information judgment unit operable to make a judgment on whether decrypted information is appropriate or not, when the decryption succeeds in the decryption trial unit; and

a terminal judgment unit operable to judge that said another terminal apparatus is a terminal apparatus of an authorized member of the group, when the information judgment unit judges that the decrypted information is appropriate.

2. The terminal apparatus according Claim 1,

wherein the inquiry information sending unit further adds, to the inquiry information, identification information for identifying the terminal apparatus, and sends the inquiry information added with said identification information; and

the information judgment unit further judges whether or not the decrypted information includes said identification information, when making the judgment on whether the decrypted information is appropriate or not.

3. The terminal apparatus according to Claim 2,

wherein the inquiry information sending unit further adds, to the inquiry information, information indicating that a user of the terminal apparatus wishes to join the group, and sends the inquiry information added with said information,

the information judgment unit further judges whether or not the decrypted information includes information indicating that the user of the terminal apparatus is approved to join the group, and

the terminal judgment unit further judges that the user of the terminal apparatus has joined the group, when the information judgment unit judges that the decrypted information includes the information indicating that the user of the terminal apparatus is approved to join the group.

4. The terminal apparatus according to Claim 2,

wherein the inquiry information sending unit further adds an arbitrary character string to the inquiry information, and sends the inquiry information added with said character string,

the information judgment unit further judges whether or not the decrypted information includes said character string and a participation certificate allowing a user of said another terminal apparatus to participate in the group, and

the terminal judgment unit further judges that said another terminal apparatus is a terminal apparatus of an authorized member of the group, when the information judgment unit judges that the decrypted information includes the character string and the participation certificate.

5. The terminal apparatus according to Claim 4,

wherein the participation certificate includes a specified expiration date,

the information judgment unit further judges whether the participation certificate included in the decrypted information is valid or not on the basis of said expiration date, and

the terminal judgment unit further judges that said another terminal apparatus is a terminal apparatus of an authorized member of the group, when the information judgment unit judges that the participation certificate is valid.

6. The terminal apparatus according to Claim 2,

wherein the inquiry information sending unit further adds an arbitrary character string to the inquiry information, and sends the inquiry information added with said character string,

the information judgment unit further judges whether the decrypted information includes said character string, a specified participation certificate, and a specified participation certificate issue permit, and

the terminal judgment unit further judges that said another terminal apparatus is a terminal apparatus of an authorized member of the group, when the information judgment unit judges that the decrypted information includes the character string, the participation certificate, and the participation certificate issue permit.

7. The terminal apparatus according to Claim 6,

wherein each of the participation certificate and the participation certificate issue permit includes a specified expiration date individually,

the information judgment unit further judges whether the participation certificate and the participation certificate issue permit included in the decrypted information are valid or not on the basis of said individual expiration date, and

the terminal judgment unit further judges that said another

terminal apparatus is a terminal apparatus of an authorized member of the group, when the information judgment unit judges that both the participation certificate and the participation certificate issue permit are valid.

8. A terminal apparatus that communicates with another terminal apparatus on a network, comprising:

an inquiry information sending unit operable to send inquiry information to said another terminal apparatus, the inquiry information indicating that a user of the terminal apparatus whishes to obtain group information including a public key of a group formed on the network;

a group information receiving unit operable to receive, from said another terminal apparatus, the group information on which a digital signature is created, in response to the inquiry information sent by the inquiry information sending unit;

a group information verification unit operable to verify validity of the received group information, using the public key included in said group information; and

a group information judgment unit operable to judge that the group information has been obtained from a terminal apparatus of an authorized member of the group, when the validity of the group information is verified by the group information verification unit.

9. The terminal apparatus according to one of Claims 1 and 8, wherein the network is a P2P network.

10. A communication method for a first terminal to communicate with a second terminal on a network, wherein the first terminal possesses a public key of a group formed on the network, the communication method comprising:

an inquiry information sending step of sending inquiry

information to the second terminal, the inquiry information indicating an inquiry about whether or not the second terminal is a terminal of an authorized member of the group;

an encrypted information receiving step of receiving predetermined encrypted information from the second terminal in response to the inquiry information sent in the inquiry information sending step;

a decryption trial step of trying decrypting the received encrypted information using the group public key;

an information judgment step of making a judgment on whether decrypted information is appropriate or not, when the decryption succeeds in the decryption trial step; and

a terminal judgment step of judging that the second terminal is a terminal of an authorized member of the group, when the decrypted information is judged to be appropriate in the information judgment step.

11. The communication method according to Claim 10,

wherein, in the inquiry information sending step, identification information for identifying the first terminal is added to the inquiry information, and the inquiry information added with said identification information is sent; and

in the information judgment step, it is further judged whether or not the decrypted information includes said identification information for identifying the first terminal, when the judgment is made on whether the decrypted information is appropriate or not.

12. The communication method according to Claim 11,

wherein, in the inquiry information sending step, information indicating that a user of the first terminal wishes to join the group is added to the inquiry information, and the inquiry information added with said information is sent,

in the information judgment step, it is further judged whether or not the decrypted information includes information indicating that the user of the first terminal is approved to join the group, and

in the terminal judgment step, it is further judged that the user of the first terminal has joined the group, when the decrypted information is judged, in the information judgment step, to include the information indicating that the user of the first terminal is approved to join the group.

13. The communication method according to Claim 11,

wherein, in the inquiry information sending step, an arbitrary character string is further added to the inquiry information, and the inquiry information added with said character string is sent,

in the information judgment step, it is further judged whether or not the decrypted information includes said character string and a participation certificate allowing a user of the second terminal to participate in the group, and

in the terminal judgment step, it is further judged that the second terminal is a terminal of an authorized member of the group, when the decrypted information is judged, in the information judgment step, to include the character string and the participation certificate.

14. The communication method according to Claim 13,

wherein the participation certificate includes a specified expiration date,

in the information judgment step, it is further judged whether or not the participation certificate included in the decrypted information is valid or not on the basis of said expiration date, and

in the terminal judgment step, it is further judged that the second terminal is a terminal of an authorized member of the group, when the participation certificate is judged to be valid in the

information judgment step.

15. The communication method according to Claim 11,

wherein, in the inquiry information sending step, an arbitrary character string is further added to the inquiry information, and the inquiry information added with said character string is sent,

in the information judgment step, it is further judged whether or not the decrypted information includes said character string, a specified participation certificate, and a specified participation certificate issue permit, and

in the terminal judgment step, it is further judged that the second terminal is a terminal of an authorized member of the group, when the decrypted information is judged, in the information judgment step, to include the character string, the participation certificate, and the participation certificate issue permit.

16. The communication method according to Claim 15,

wherein each of the participation certificate and the participation certificate issue permit includes a specified expiration date individually,

in the information judgment step, it is further judged whether the participation certificate and the participation certificate issue permit included in the decrypted information are valid or not on the basis of said individual expiration date, and

in the terminal judgment step, it is further judged that the second terminal is a terminal of an authorized member of the group, when both the participation certificate and the participation certificate issue permit are judged to be valid in the information judgment step.

17. A communication method for a first terminal that communicates with a second terminal on a network, comprising:

an inquiry information sending step of sending inquiry information to the second terminal, the inquiry information indicating that a user of the first terminal whishes to obtain group information including a public key of a group formed on the network;

a group information receiving step of receiving, from the second terminal, the group information on which a digital signature is created, in response to the inquiry information sent in the inquiry information sending step;

a group information verification step of verifying validity of the received group information, using the public key included in said group information; and

a group information judgment step of judging that the group information has been obtained from a terminal of an authorized member of the group, when the validity of the group information is verified in the group information verification step.

18. The communication method according to one of Claims 10 and 17,

wherein the network is a P2P network.

19. A communication method for carrying out a communication between a first terminal and a second terminal on a network, wherein the first terminal possesses a public key of a group formed on the network and a pair of a private key and a public key of a first user who is a user of the first terminal, and the second terminal possesses a pair of a private key and a public key of the group, the communication method comprising steps A executed by the first terminal and steps B executed by the second terminal,

wherein the steps A include:

an inquiry information sending step of sending inquiry information to the second terminal, the inquiry information indicating an inquiry about whether or not the second terminal is a

terminal of an authorized member of the group;

an encrypted information receiving step of receiving predetermined encrypted information from the second terminal in response to the inquiry information sent in the inquiry information sending step;

a decryption trial step of trying decrypting the received encrypted information using the group public key;

an information judgment step of making a judgment on whether decrypted information is appropriate or not, when the decryption succeeds in the decryption trial step;

a manager judgment step of judging that the second terminal is a terminal of an authorized manager of the group, when the decrypted information is judged to be appropriate in the information judgment step;

a membership request sending step of sending membership request information to the second terminal judged to be the authorized manager in the manager judgment step, the membership request information including information indicating that the first user wishes to join the group and the pubic key of the first user; and

a participation certificate receiving step of receiving a participation certificate indicating that the first user has been approved to join the group from the second terminal, and

the steps B include:

an inquiry information receiving step of receiving the inquiry information from the first terminal;

an encrypted information sending step of generating the encrypted information which has been encrypted according to the received inquiry information, and sending the generated encrypted information to the first terminal;

a membership request receiving step of receiving the membership request information from the first terminal;

a participation certificate generation step of generating the

participation certificate on the basis of the received membership request information; and

a participation certificate sending step of sending the generated participation certificate to the first terminal.

20. The communication method according to Claim 19,

wherein the steps B further include:

a request date specification step of specifying a date, month and year on which the membership request information was received; and

an expiration date determination step of determining an expiration date of the participation certificate on the basis of said specified date, month, and year, and

in the participation certificate generation step, the participation certificate is generated according to the membership request information and said expiration date.

21. A communication method for carrying out a communication between a first terminal and a second terminal on a network, wherein the first terminal possesses a pair of a private key and a public key of a group formed on the network and a public key of a second user who is a user of the second terminal, and the second terminal possesses a public key of the group, the communication method comprising steps A executed by the first terminal and steps B executed by the second terminal,

wherein the steps A include:

an inquiry information sending step of sending inquiry information to the second terminal, the inquiry information indicating an inquiry about whether or not the second terminal is a terminal of an authorized member of the group;

an encrypted information receiving step of receiving predetermined encrypted information from the second terminal in

response to the inquiry information sent in the inquiry information sending step;

a decryption trial step of trying decrypting the received encrypted information using the group public key of the second user;

an information judgment step of making a judgment on whether decrypted information is appropriate or not, when the decryption succeeds in the decryption trial step;

a participant judgment step of judging that the second terminal is a terminal of an authorized participant in the group, when the decrypted information is judged to be appropriate in the information judgment step;

an assignment information sending step of sending assignment information to the second terminal whose user, that is, the second user is judged to be an authorized participant, the assignment information indicating that said second user is wished to be assigned as an issuer of the group who issues a participation certificate;

a public key receiving step of receiving the public key of the second user from the second terminal;

a public key judgment step of judging whether or not the received public key of the second user and the public key possessed by the first terminal match;

a permit generation step of generating a participation certificate issue permit indicating that authority to issue the participation certificate is granted to the second user; and

a permit sending step of sending the generated participation certificate issue permit to the second terminal, and

the steps B include:

an inquiry information receiving step of receiving the inquiry information from the first terminal;

a public key sending step of sending the public key of the

second user to the first terminal; and

a permit receiving step of receiving the participation certificate issue permit from the first terminal.

22. The communication method according to Claim 21,

wherein the steps A further include:

a permission date specification step of specifying a date, month and year on which the public key of the second user was received; and

an expiration date determination step of determining an expiration date of the participation certificate issue permit, on the basis of said specified date, month, and year, and

in the permit generation step, the participation certificate issue permit is generated according to the public key of the second user and said expiration date.

23. A communication method for carrying out a communication between a first terminal and a second terminal on a network, wherein the first terminal possesses a public key of a group formed on the network and a pair of a private key and a public key of a first user who is a user of the first terminal, and the second terminal possesses a public key of the group, the communication method comprising steps A executed by the first terminal and steps B executed by the second terminal,

wherein the steps A include:

an inquiry information sending step of sending inquiry information to the second terminal, the inquiry information indicating an inquiry about whether or not the second terminal is a terminal of an authorized issuer of the group who has authority to issue a participation certificate;

a permit receiving step of receiving an encrypted participation certificate issue permit from the second terminal;

a decryption trial step of trying decrypting the received participation certificate issue permit using the public key of the group;

an information judgment step of making a judgment on whether decrypted participation certificate issue permit is appropriate or not, when the decryption succeeds in the decryption trial step;

an issuer judgment step of judging that the second terminal is a terminal of an authorized issuer of the group, when the decrypted participation certificate issue permit is judged to be appropriate in the information judgment step;

a membership request sending step of sending membership request information to the second terminal judged to be the authorized issuer in the issuer judgment step, the membership request information including information indicating that the first user wishes to join the group and the pubic key of the first user; and

a participation certificate receiving step of receiving a participation certificate indicating that the first user has been approved to join the group from the second terminal, and

the steps B include:

an inquiry information receiving step of receiving the inquiry information from the first terminal;

an encrypted information sending step of sending the encrypted participation certificate issue permit to the first terminal after the inquiry information is received;

a membership request receiving step of receiving the membership request information from the first terminal;

a participation certificate generation step of generating the participation certificate on the basis of the received membership request information; and

a participation certificate sending step of sending the generated participation certificate to the first terminal.

24. The communication method according to Claim 23,

wherein the steps B further include:

a request date specification step of specifying a date, month and year on which the membership request information was received; and

an expiration date determination step of determining an expiration date of the participation certificate on the basis of said specified date, month, and year, and

in the participation certificate generation step, the participation certificate is generated according to the membership request information and said expiration date.

25. The communication method according to one of Claims 19, 21, and 23,

wherein the network is a P2P network.

26. A communication system comprising a first terminal and a second terminal that communicate with each other on a network, the first terminal possessing a public key of a group formed on the network and a pair of a private key and a public key of a first user who is a user of the first terminal, and the second terminal possessing a pair of a private key and a public key of the group,

wherein the first terminal includes:

an inquiry information sending unit operable to send inquiry information to the second terminal, the inquiry information indicating an inquiry about whether or not the second terminal is a terminal of an authorized member of the group;

an encrypted information receiving unit operable to receive predetermined encrypted information from the second terminal in response to the inquiry information sent by the inquiry information sending unit;

a decryption trial unit operable to try decrypting the received encrypted information using the group public key;

an information judgment unit operable to make a judgment on whether decrypted information is appropriate or not, when the decryption succeeds in the decryption trial unit;

a manager judgment unit operable to judge that the second terminal is a terminal of an authorized manager of the group, when the information judgment unit judges that the decrypted information is appropriate;

a membership request sending unit operable to send membership request information to the second terminal judged to be the authorized manager by the manager judgment unit, the membership request information including information indicating that the first user wishes to join the group and the pubic key of the first user; and

a participation certificate receiving unit operable to receive a participation certificate indicating that the first user has been approved to join the group from the second terminal, and

the second terminal includes:

an inquiry information receiving unit operable to receive the inquiry information from the first terminal;

an encrypted information sending unit operable to generate the encrypted information which has been encrypted according to the received inquiry information, and send the generated encrypted information to the first terminal;

a membership request receiving unit operable to receive the membership request information from the first terminal;

a participation certificate generation unit operable to generate the participation certificate on the basis of the received membership request information; and

a participation certificate sending unit operable to send the generated participation certificate to the first terminal.

27. The communication system according to Claim 26,

wherein the second terminal further includes:

a request date specification unit operable to specify a date, month and year on which the membership request information was received; and

an expiration date determination unit operable to determine an expiration date of the participation certificate on the basis of the specified date, month, and year, and

the participation certificate generation unit generates the participation certificate according to the membership request information and said expiration date.

28. A communication system comprising a first terminal and a second terminal that communicate with each other on a network, the first terminal possessing a pair of a private key and a public key of a group formed on the network and a public key of a second user who is a user of the second terminal, and the second terminal possessing a public key of the group,

wherein the first terminal includes:

an inquiry information sending unit operable to send inquiry information to the second terminal, the inquiry information indicating an inquiry about whether or not the second terminal is a terminal of an authorized member of the group;

an encrypted information receiving unit operable to receive predetermined encrypted information from the second terminal in response to the inquiry information sent by the inquiry information sending unit;

a decryption trial unit operable to try decrypting the received encrypted information using the public key of the second user;

an information judgment unit operable to make a judgment on whether decrypted information is appropriate or not, when the

decryption succeeds in the decryption trial unit;

a participant judgment unit operable to judge that the second terminal is a terminal of an authorized participant in the group, when the information judgment unit judges that the decrypted information is appropriate;

an assignment information sending unit operable to send assignment information to the second terminal whose user, that is, the second user is judged to be an authorized participant, the assignment information indicating that the second user is wished to be assigned as an issuer of the group who issues a participation certificate;

a public key receiving unit operable to receive the public key of the second user from the second terminal;

a public key judgment unit operable to judge whether or not the received public key of the second user and the public key possessed by the first terminal match;

a permit generation unit operable to generate a participation certificate issue permit indicating that authority to issue the participation certificate is granted to the second user; and

a permit sending unit operable to send the generated participation certificate issue permit to the second terminal, and

the second terminal includes:

an inquiry information receiving unit operable to receive the inquiry information from the first terminal;

a public key sending unit operable to send the public key of the second user to the first terminal; and

a permit receiving unit operable to receive the participation certificate issue permit from the first terminal.

29. The communication system according to Claim 28,

wherein first terminal further includes:

a permission date specification unit operable to specify a date,

month and year on which the public key of the second user was received; and

an expiration date determination unit operable to determine an expiration date of the participation certificate issue permit, on the basis of said specified date, month, and year, and

the permit generation unit generates the participation certificate issue permit according to the public key of the second user and said expiration date.

30. A communication system comprising a first terminal and a second terminal that communicate with each other on a network, the first terminal possessing a public key of a group formed on the network and a pair of a private key and a public key of a first user who is a user of the first terminal, and the second terminal possessing a public key of the group,

wherein the first terminal includes:

an inquiry information sending unit operable to send inquiry information to the second terminal, the inquiry information indicating an inquiry about whether or not the second terminal is a terminal of an authorized issuer of the group who has authority to issue a participation certificate;

a permit receiving unit operable to receive an encrypted participation certificate issue permit from the second terminal;

a decryption trial unit operable to try decrypting the received participation certificate issue permit using the public key of the group;

an information judgment unit operable to make a judgment on whether decrypted participation certificate issue permit is appropriate or not, when the decryption succeeds in the decryption trial unit;

an issuer judgment unit operable to judge that the second terminal is a terminal of an authorized issuer of the group, when the

information judgment unit judges that the decrypted participation certificate issue permit is appropriate;

a membership request sending unit operable to send membership request information to the second terminal judged to be the authorized issuer by the issuer judgment unit, the membership request information including information indicating that the first user wishes to join the group and the pubic key of the first user; and

a participation certificate receiving unit operable to receive a participation certificate indicating that the first user has been approved to join the group from the second terminal, and

the second terminal includes:

an inquiry information receiving unit operable to receive the inquiry information from the first terminal;

an encrypted information sending unit operable to send the encrypted participation certificate issue permit to the first terminal after receiving the inquiry information;

a membership request receiving unit operable to receive the membership request information from the first terminal,

a participation certificate generation unit operable to generate the participation certificate on the basis of the received membership request information; and

a participation certificate sending unit operable to send the generated participation certificate to the first terminal.

31. The communication system according to Claim 30,

wherein the second terminal further includes:

a request date specification unit operable to specify a date, month and year on which the membership request information was received; and

an expiration date determination unit operable to determine an expiration date of the participation certificate on the basis of said

specified date, month, and year, and

the participation certificate generation unit generates the participation certificate according to the membership request information and said expiration date.

32. The communication system according to one of Claims 26, 28, and 30,

wherein the network is a P2P network.

33. A program for a terminal apparatus that communicates with another terminal apparatus on a network, wherein the first terminal apparatus possesses a public key of a group formed on the network, the program comprising:

an inquiry information sending step of sending inquiry information to said another terminal apparatus, the inquiry information indicating an inquiry about whether or not said another terminal apparatus is a terminal apparatus of an authorized member of the group;

an encrypted information receiving step of receiving predetermined encrypted information from said another terminal apparatus in response to the inquiry information sent in the inquiry information sending step;

a decryption trial step of trying decrypting the received encrypted information using the group public key;

an information judgment step of making a judgment on whether decrypted information is appropriate or not, when the decryption succeeds in the decryption trial step; and

a terminal judgment step of judging that said another terminal apparatus is a terminal apparatus of an authorized member of the group, when the decrypted information is judged to be appropriate in the information judgment step.

34. The program according to Claim 33, wherein the network is a P2P network.